OFFICE OF
Privacy Protection

2/1/06

Identity Theft Victim Checklist

CONSUMER INFORMATION SHEET 3

This checklist can help identity theft victims clear up their records. It lists the actions most identity theft victims should take to limit the damage done by the thief. For more information, see the Web sites of the Federal Trade Commission at www.consumer.gov/idtheft, the Identity Theft Resource Center at www.idtheftcenter.org, and the Privacy Rights Clearinghouse at www.privacyrights.org.

Report the fraud to the three major credit bureaus.

You can report the identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system and you will not be able to speak to anyone at this time. The system will ask you to enter your Social Security number and other information to identify yourself. The automated system allows you to flag your file with a fraud alert at all three bureaus. This helps stop a thief from opening new accounts in your name. The alert stays on for 90 days. Each of the credit bureaus will send you a letter confirming your fraud alert and giving instructions on how to get a copy of your credit report. As a victim of identity theft, you will not be charged for these reports. Each report you receive will contain a telephone number you can call to speak to someone in the credit bureau's fraud department.

Experian 1-888-397-3742 Equifax 1-800-525-6285 TransUnion 1-800-680-7289

Report the crime to the police.

Under California law, you can report identity theft to your local police department. Ask the police to issue a police report of identity theft. Give the police as much information on the theft as possible. One way to do this is to provide copies of your credit reports showing the items related to identity theft. Black out other items not related to identity theft. Give the police any new evidence you collect to add to your report. Be sure to get a copy of your police report. You will need to give copies to creditors and the credit bureaus. For more information, see "Organizing Your Identity Theft Case" by the Identity Theft Resource Center, available at www.idtheftcenter.org/vg106.shtml.

Request information on fraudulent accounts.

When you file your police report of identity theft, the officer may give you forms to use to request account information from credit grantors, utilities or cell phone service companies. If the officer does not do this, you can use the form available from the Office of Privacy Protection in Consumer Information Sheet 3A, "Requesting Information on Fraudulent Accounts." When you write to creditors where the thief opened or applied for accounts, send copies of the forms, along with copies of the police report. Give the information you receive from creditors to the officer investigating your case.

Call creditors.

Call creditors for any accounts that the thief opened or used. When you call, ask for the security or fraud department. Examples of creditors are credit card companies, other lenders, phone companies, other utility companies, and department stores. Tell them you are an identity theft victim. Ask them not to hold you responsible for *new accounts* opened by the thief.

If your *existing credit accounts* have been used fraudulently, ask the credit issuers to close those accounts and to report them to credit bureaus as "closed at consumer's request." If you open a new account, have it set up to require a password or PIN to approve use. Don't use your mother's maiden name or the last four numbers of your Social Security number as your password. Ask the creditors to give you copies of documentation on the fraudulent accounts (see above item). For more information on what to tell creditors, see the Federal Trade Commission's identity theft Web site at www.consumer.gov/idtheft.

Review your credit reports carefully.

When you receive your credit reports, read them carefully. Look for accounts you don't recognize. Look in the inquiries section for names of creditors from whom you haven't requested credit. You may find some inquiries identified as "promotional." These occur when a company has gotten your name and address from a credit bureau to send you an offer of credit. Promotional inquiries are not signs of fraud. (By calling to report identity theft, your name will be automatically removed from the mailing list to receive unsolicited credit offers of this kind.) Also, as a general precaution, look in the personal information section to verify your Social Security number, address and name.

If you find anything you don't understand, call the credit bureau at the telephone number listed on the report. Tell them you want to block, or remove, any information on the report that is the result of identity theft. (You must send a police report of identity theft to support this request.) Order new credit reports every three months or so until your situation has cleared up. You may have to pay $8 or $9 for each report, but ask for additional free copies as an identity theft victim. For more on what to tell the credit bureaus, see the Privacy Rights Clearinghouse's "Identity Theft: What to Do When It Happens to You" at www.privacyrights.org/fs/fs17a.htm.

Use the ID Theft Affidavit.

Creditors may ask you to fill out fraud affidavits. The Federal Trade Commission's ID Theft Affidavit is accepted by the credit bureaus and by most major creditors. Send copies of the completed form to creditors where the thief opened accounts in your name. Also send copies to creditors where the thief made charges on your account, to the credit bureaus, and to the police. The form is available on the FTC Web site at www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf. File a complaint of identity theft with the FTC. See their Web site at www.consumer.gov/idtheft. The FTC keeps a database of identity theft cases that is used by many law enforcement agencies.

Write to the credit bureaus.

Write a letter to each credit bureau. Repeat what you said in your telephone call (see above). Send copies of your police report and completed ID Theft Affidavit. Remind the credit bureaus that they must block or remove any information that you, as an identity theft victim, say is a

result of the theft. Send your letters by certified mail, return receipt requested. Keep a copy of each letter. See the Sample Letter to Credit Bureaus on page 5.

Equifax	Experian	TransUnion
P.O Box 740241	P.O. Box 9532	P.O. Box 6790
Atlanta, GA 30374-0241	Allen, TX 75013	Fullerton, CA 92834

As an alternative, you may dispute items with the credit bureaus online. Look for "dispute" on their Web sites: www.equifax.com, www.experian.com, and www.transunion.com.

Write to creditors.

Write a letter to each creditor where an account was opened or used in your name. Repeat what you said in your telephone call. Send a copy of your police report. Black out the account number of any accounts with other creditors on a copy of your completed ID Theft Affidavit and send it. See the Sample Letter to Creditor on Existing Account on page 6 and Sample Letter to Creditor on New Account on page 7.

If your checks, ATM card or bank account information are lost or stolen...

Call the bank and close your bank account. Open a new one with a new account number. Tell the bank you want to use a new password for access to your new account. Do not use your mother's maiden name or the last four digits of your Social Security number. Ask your bank to notify the check verification company it uses. Report the stolen checks to the check verification companies that retail stores use. You can also contact major check verification companies. Ask them to notify retailers who use their databases not to accept the checks on your closed account. Call TeleCheck at 1-800-710-9898 and Certegy, Inc. at 1-800-437-5120. To find out if the identity thief has passed bad checks in your name, call SCAN at 800-262-7771. Follow up by writing to your bank. Send your letter by certified mail, return receipt requested.

If you are contacted by a debt collector...

Tell the debt collector that you are the victim of identity theft. Say that you dispute the validity of the debt. Say that you did not create the debt and are not responsible for it. Send the collector a follow-up letter saying the same things. Include a copy of your police report and of any documents you've received from the creditor. Write in your letter that you are giving notice to a claimant under California Civil Code section 1798.93, subsection (c)(5) that a situation of identity theft exists. Send the letter by certified mail, return receipt requested. If the debt collector is not the original creditor, be sure to send your letter within 30 days of receiving the collector's first written demand for payment.

If your driver license or DMV-issued ID card is stolen...

Immediately contact your local DMV office to report the theft. Ask them to put a fraud alert on your license. Then call the toll-free DMV Fraud Hotline at 866-658-5758. If the thief is using your license as ID, you may want to change your license number. Ask DMV for an appointment. Take a copy of the police report and copies of bills or other items supporting your claim of fraud. You will also need to prove your identity. Take current documents such as a passport, a

certification of citizenship or naturalization, or a U.S. military photo ID. DMV will issue a new driver license or ID card number when you meet all the requirements.

If your mail was stolen or your address changed by an identity thief...

Notify the Postal Inspector if you think an identity thief has stolen your mail or filed a change of address request in your name. To find the nearest Postal Inspector, look in the white pages of the telephone book for the Post Office listing under United States Government. Or go to the Postal Inspection Service's Web site at www.usps.com/websites/depart/inspect.

If you are wrongly accused of a crime committed by an identity thief...

"Criminal identity theft" is a label given to a particular type of identity theft. Criminal identity theft occurs when a suspect in a criminal investigation identifies himself or herself using the identity of another, innocent person. A special database in the California Department of Justice can help victims of this kind of identity theft. See the Office of Privacy Protection's Consumer Information Sheet 8: "How to Use the California Identity Theft Registry - A Guide for Victims of 'Criminal' Identity Theft," available on our Identity Theft Web page at http://www.privacy.ca.gov/cover/identitytheft.htm.

If someone uses your Social Security number to claim unemployment benefits or to work...

If you suspect that someone else has claimed unemployment benefits using your Social Security number, call the California Employment Development Department's toll-free Fraud Hotline at 800-229-6297. For more information, see their Web site at www.edd.ca.gov. Sometimes, an identity thief will use someone else's Social Security number to be eligible to work. It's a good idea to check your Social Security earnings record to see if a thief is using your Social Security number. You can get a copy of your earnings record by calling 1-800-772-1213. Or get a Request for Social Security Statement (Form 7004) at www.ssa.gov/online/ssa-7004.html. If a thief is using your Social Security number, call the Social Security Fraud Hotline at 1-800-269-0271. You can also read "Identity Theft and Your Social Security Number," at www.ssa.gov/pubs/10064.html.

OFFICE OF
Privacy Protection

Your Social Security Number: Controlling the Key to Identity Theft

CONSUMER INFORMATION SHEET 4

Your Social Security number is the key.

Originally, your Social Security number (SSN) was a way for the government to track your earnings and pay you retirement benefits. But over the years, it has become much more than that. It is the key to a lot of your personal information.

With your SSN, an identity thief can get your credit history, your bank account, your charge accounts, and your utility accounts. A thief can also use the number to open new credit and bank accounts or to get a driver's license—all using your identity.

Don't carry your Social Security card in your wallet.

You don't need to have your Social Security card with you at all times. Keep it at home in a safe place. Check for other cards that may have your SSN on them.

Ask questions when they ask for your Social Security number.

There is no law that prevents businesses from asking for your SSN. And you may be denied service if you don't give the number. If giving your SSN to a business doesn't seem reasonable to you, ask if you can show another form of identification. Or ask if the business can use another number as your customer number.

Remember that some government agencies can require your SSN. These agencies include DMV, welfare offices, and tax agencies. Look for the required "disclosure" form. The form should state if giving the number is required or optional, how it will be used, and the agency's legal authority to ask for it.[1]

California law limits the public display of Social Security numbers.

A California law bars many organizations from publicly displaying SSNs.[2]

The law prohibits:

- Printing SSNs on ID cards or badges,
- Printing SSNs on documents mailed to customers, unless the law requires it or the document is a form or application,
- Printing SSNs on postcards or any other mailer where its visible without opening an envelope,

- Avoiding legal requirements by encoding or embedding SSNs in cards or documents, such as using a bar code, chip or magnetic strip,
- Requiring people to send SSNs over the Internet, unless the connection is secure or the number is encrypted, and
- Requiring people to use an SSN to log onto a web site, unless a password is also used.

The law applies to businesses, government and other entities.

Ask your companies to change now.

Organizations may continue their current practices for using SSNs for existing customers, rather than stopping the practices barred by the new law described above—unless a customer requests otherwise in writing. You can ask a company or organization to treat your SSN as the law requires now. Send a letter that says something like the following: "I am hereby requesting that you comply with the requirements of California Civil Code section 1798.85 related to your use of my Social Security number. I understand that you have 30 days from the receipt of this letter to comply."

IMPORTANT NOTE: Health care providers, health plans and insurance companies are given more time to comply with the ban on printing SSNs on ID cards. They must fully comply by July 2005.

Getting a new Social Security number is probably not a good idea.

Victims of identity theft sometimes want to change their Social Security number. The Social Security Administration very rarely allows this. In fact, there are drawbacks to changing your number. It could result in losing your credit history, your academic records, and your professional degrees. The absence of any credit history under the new SSN would make it difficult for you to get credit, rent an apartment, or open a bank account.

Here's where to get more information on Social Security numbers.

Identity Theft: If you think an identity thief is using your SSN, call the Social Security Fraud Hotline at 1-800-269-0271. If you think someone may be using your SSN to work, check your Social Security Personal Earnings and Benefit Statement. You can get a copy by calling 1-800-772-1213, or online at www.ssa.gov/online/ssa-7004.pdf. Also see the Social Security Administration's booklet "When Someone Misuses Your Number," available at www.ssa.gov/pubs/10064.html.

What the Numbers Mean: For an explanation of the meaning of the numbers in SSNs, see "Structure of Social Security Numbers," by Computer Professionals for Social Responsibility, available at http://www.cpsr.org/issues/privacy/SSNStructure/.

More on Protecting Your SSN: "Fact Sheet 10: My Social Security Number: How Secure Is It?" by the Privacy Rights Clearinghouse, available at www.privacyrights.org/fs/fs10-ssn.htm.

Recommended Practices: For recommendations on how organizations can protect privacy in their handling of SSNs, see the Office of Privacy Protection's "Recommended Practices for Protecting the Confidentiality of Social Security Numbers," available on the Recommended Practices Web page at www.privacy.ca.gov.

NOTES

[1] The federal Privacy Act of 1974, 5 U.S. Code 552a, is available on the Privacy Laws Web page at http://www.privacy.ca.gov/.
[2] California Civil Code section 1798.85 can be found on the Office of Privacy Protection's Privacy Laws page at http://www.privacy.ca.gov/.

OFFICE OF
Privacy
Protection

Top 10 Tips for Identity Theft Protection

CONSUMER INFORMATION SHEET 1

An identity thief takes your personal information and uses it without your knowledge. The thief may run up debts or even commit crimes in your name. The following tips can help you lower your risk of becoming a victim.

Protect your Social Security number.

Don't carry your Social Security card in your wallet. If your health plan (other than Medicare) or another card uses your Social Security number, ask the company for a different number. For more information, see "Your Social Security Number: Controlling the Key to Identity Theft" (Consumer Information Sheet 4) on our Social Security Numbers Web page.

Fight "phishing" – don't take the bait.

Scam artists "phish" for victims by pretending to be banks, stores or government agencies. They do this over the phone, in e-mails and in the regular mail. Don't give out your personal information – unless you made the contact. Don't respond to a request to verify your account number or password. Legitimate companies do not request this kind of information in this way.

Keep your identity from getting trashed.

Shred or tear up papers with personal information before you throw them away. Shred credit card offers and "convenience checks" that you don't use.

Control your personal financial information.

California law requires your bank and other financial services companies to get your permission before sharing your personal financial information with outside companies. You also have the right to limit some sharing of your personal information with your companies' affiliates. For more information, see "Your Financial Privacy" (Consumer Information Sheet 2) on our Financial Privacy Web page.

Shield your computer from viruses and spies.

Protect your personal information on your home computer. Use strong passwords: with at least eight characters, including a combination of letters, numbers, and symbols, easy for you to remember, but difficult for others to guess. Use firewall, virus and spyware protection software that you update regularly. Steer clear of spyware. Download free software only from sites you know and trust. Don't install software without knowing what it is. Set Internet Explorer browser security to at least "medium." Don't click on links in pop-up windows or in spam e-mail.

Click with caution

When shopping online, check out a Web site before entering your credit card number or other personal information. Read the privacy policy and look for opportunities to opt out of information sharing. (If there is no privacy policy posted, beware! Shop elsewhere.) Only enter personal information on secure Web pages with "https" in the address bar and a padlock symbol at the bottom of the browser window. These are signs that your information will be encrypted or scrambled, protecting it from hackers.

Check your bills and bank statements.

Open your credit card bills and bank statements right away. Check carefully for any unauthorized charges or withdrawals and report them immediately. Call if bills don't arrive on time. It may mean that someone has changed contact information to hide fraudulent charges.

Stop pre-approved credit offers.

Stop most pre-approved credit card offers. They make a tempting target for identity thieves who steal your mail. Have your name removed from credit bureau marketing lists. Call toll-free 888-5OPTOUT (888-567-8688).

Ask questions.

Ask questions whenever you are asked for personal information that seems inappropriate for the transaction. Ask how the information will be used and if it will be shared. Ask how it will be protected. Explain that you're concerned about identity theft. If you're not satisfied with the answers, consider going somewhere else.

Check your credit reports – for free.

One of the best ways to protect yourself from identity theft is to monitor your credit history. You can get one free credit report every year from each of the three national credit bureaus: Equifax, Experian and TransUnion. Request all three reports at once, or be your own no-cost credit-monitoring service. Just spread out your requests, ordering from a different bureau every four months. (More comprehensive monitoring services from the credit bureaus cost from $44 to over $100 per year.) Order your free annual credit reports by phone, toll-free, at 1-877-322-8228, or online at https://www.annualcreditreport.com/cra/index.jsp. Or you can mail in an order form. See our Consumer Information Sheet 10, "How to Freeze Your Credit Files."